FIG. 1

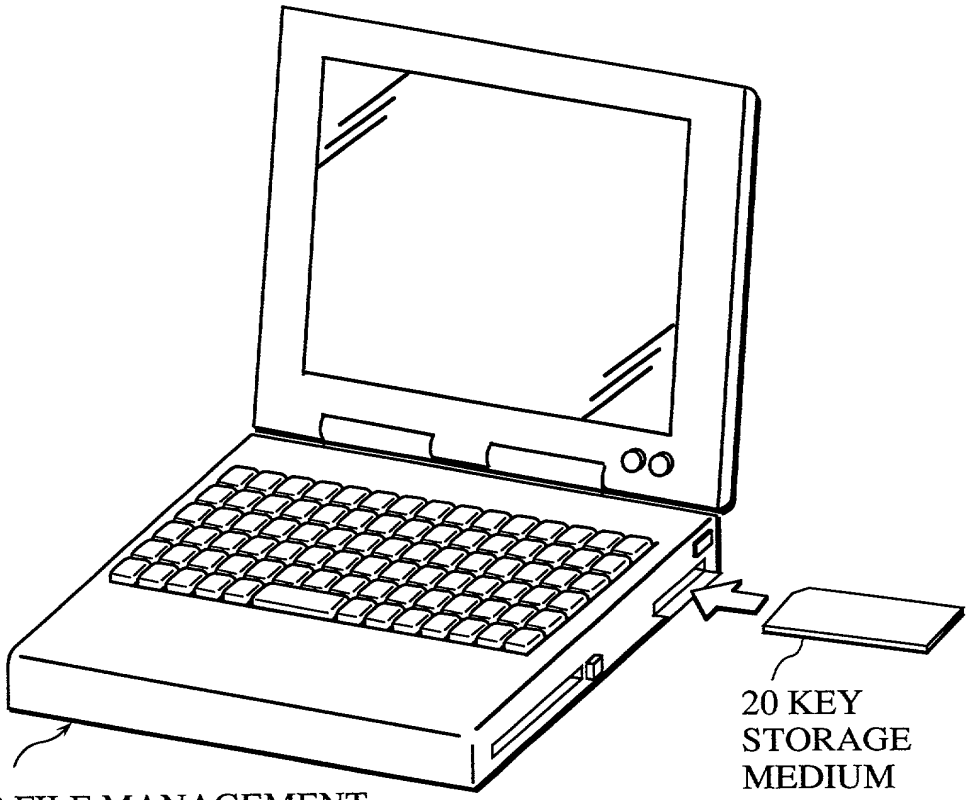


FIG. 2

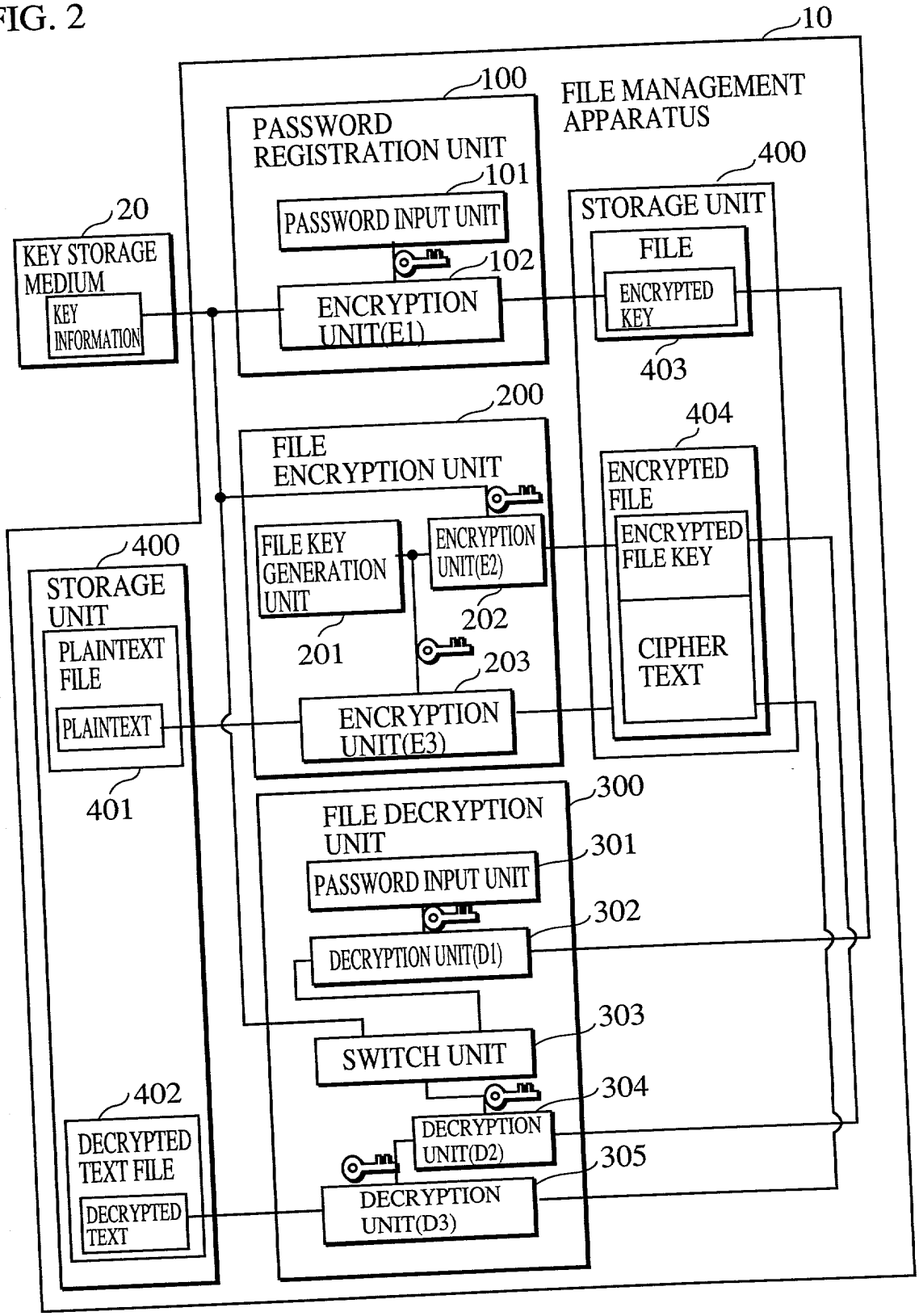

10
FILE MANAGEMENT APPARATUS
100
PASSWORD REGISTRATION UNIT
101
PASSWORD INPUT UNIT
102
ENCRYPTION UNIT(E1)
20
KEY STORAGE MEDIUM
KEY INFORMATION
400
STORAGE UNIT
FILE
ENCRYPTED KEY
403
200
FILE ENCRYPTION UNIT
404
ENCRYPTED FILE
ENCRYPTED FILE KEY
CIPHER TEXT
FILE KEY GENERATION UNIT
ENCRYPTION UNIT(E2)
201
202
203
ENCRYPTION UNIT(E3)
400
STORAGE UNIT
PLAINTEXT FILE
PLAINTEXT
401
300
FILE DECRYPTION UNIT
301
PASSWORD INPUT UNIT
302
DECRYPTION UNIT(D1)
303
SWITCH UNIT
304
DECRYPTION UNIT(D2)
305
DECRYPTION UNIT(D3)
402
DECRYPTED TEXT FILE
DECRYPTED TEXT

FIG. 3

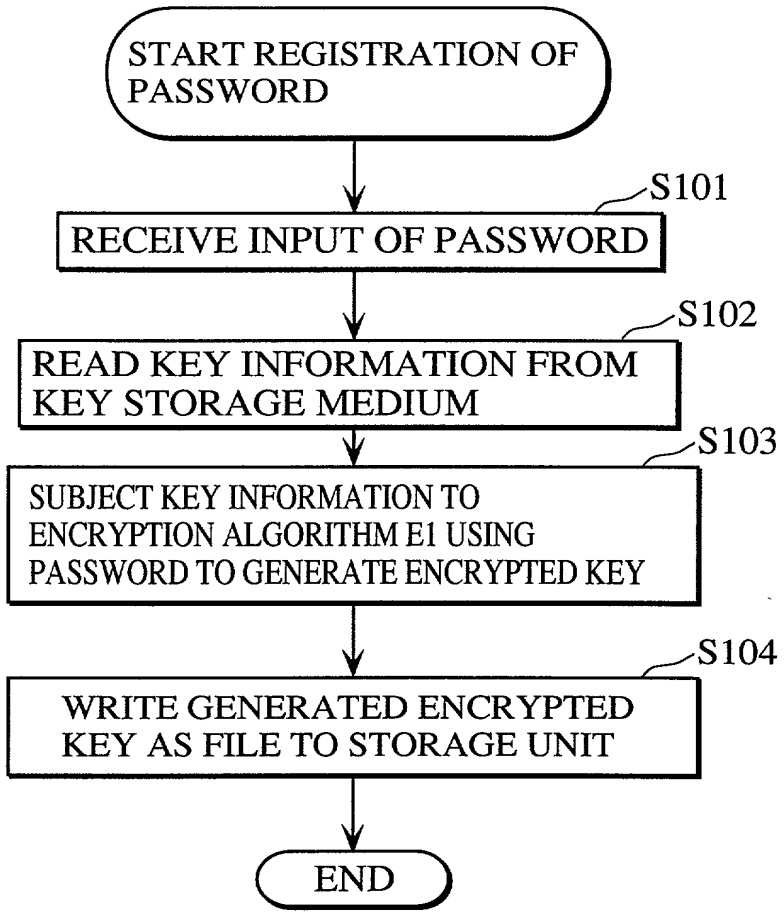

START REGISTRATION OF PASSWORD
S101
RECEIVE INPUT OF PASSWORD
S102
READ KEY INFORMATION FROM KEY STORAGE MEDIUM
S103
SUBJECT KEY INFORMATION TO ENCRYPTION ALGORITHM E1 USING PASSWORD TO GENERATE ENCRYPTED KEY
S104
WRITE GENERATED ENCRYPTED KEY AS FILE TO STORAGE UNIT
END

FIG. 4

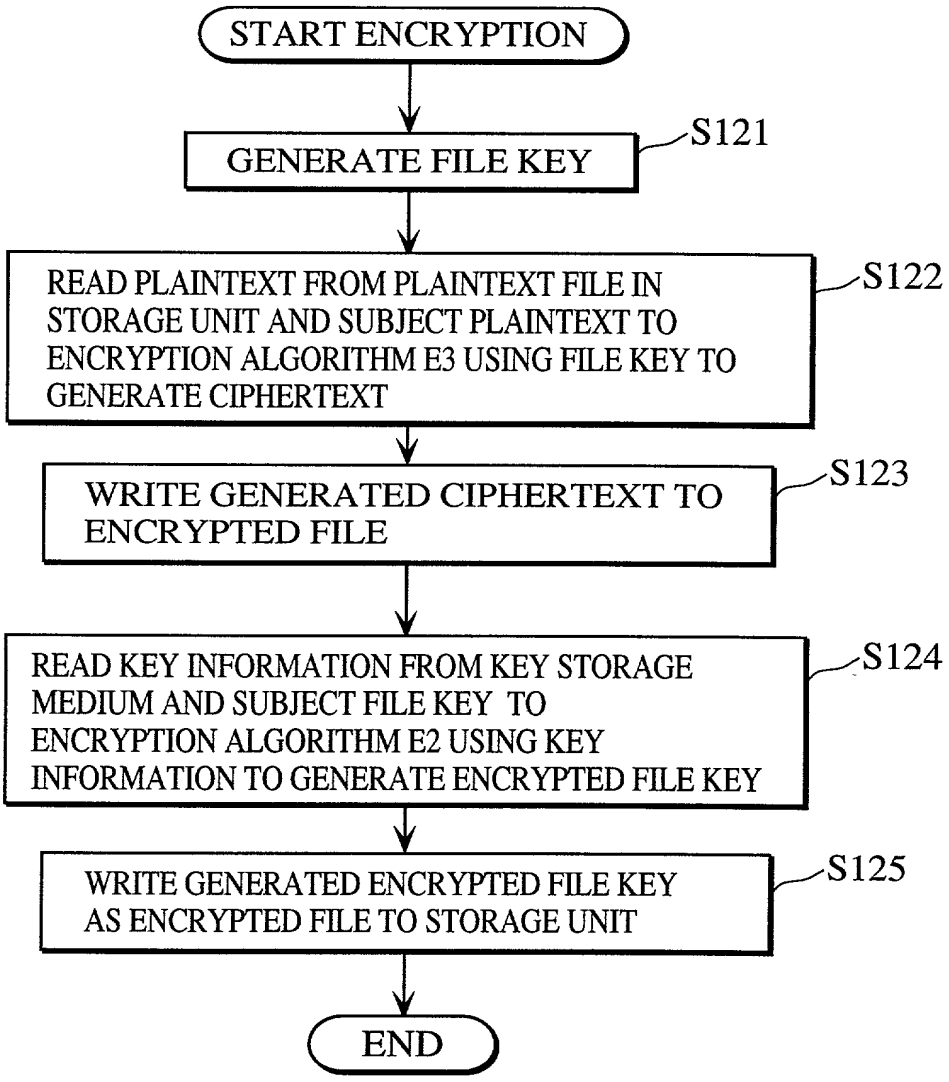

START ENCRYPTION
GENERATE FILE KEY
S121
READ PLAINTEXT FROM PLAINTEXT FILE IN STORAGE UNIT AND SUBJECT PLAINTEXT TO ENCRYPTION ALGORITHM E3 USING FILE KEY TO GENERATE CIPHERTEXT
S122
WRITE GENERATED CIPHERTEXT TO ENCRYPTED FILE
S123
READ KEY INFORMATION FROM KEY STORAGE MEDIUM AND SUBJECT FILE KEY TO ENCRYPTION ALGORITHM E2 USING KEY INFORMATION TO GENERATE ENCRYPTED FILE KEY
S124
WRITE GENERATED ENCRYPTED FILE KEY AS ENCRYPTED FILE TO STORAGE UNIT
S125
END

FIG. 5

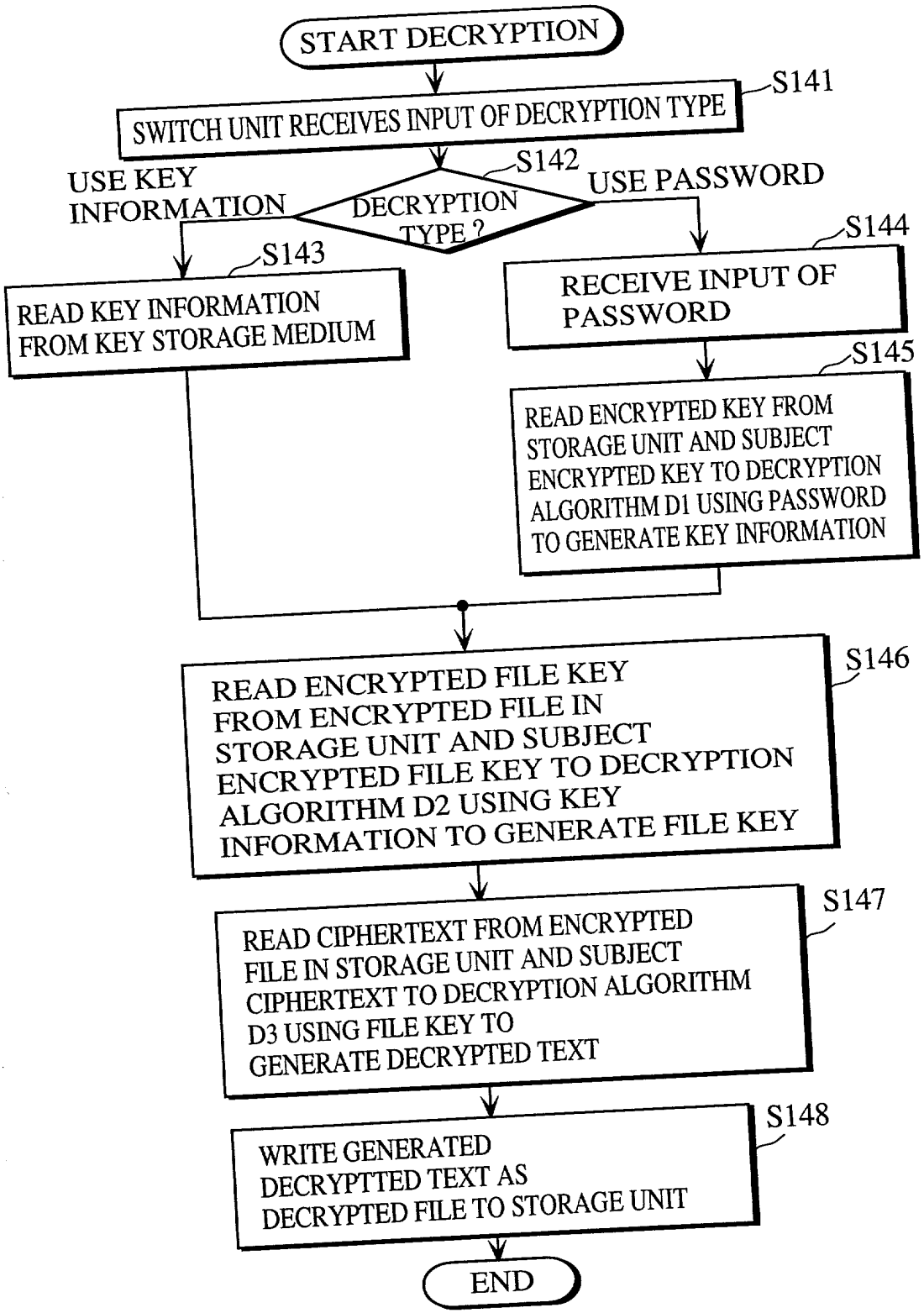

START DECRYPTION
SWITCH UNIT RECEIVES INPUT OF DECRYPTION TYPE
S141
S142
USE KEY INFORMATION
DECRYPTION TYPE ?
USE PASSWORD
S143
READ KEY INFORMATION FROM KEY STORAGE MEDIUM
S144
RECEIVE INPUT OF PASSWORD
S145
READ ENCRYPTED KEY FROM STORAGE UNIT AND SUBJECT ENCRYPTED KEY TO DECRYPTION ALGORITHM D1 USING PASSWORD TO GENERATE KEY INFORMATION
S146
READ ENCRYPTED FILE KEY FROM ENCRYPTED FILE IN STORAGE UNIT AND SUBJECT ENCRYPTED FILE KEY TO DECRYPTION ALGORITHM D2 USING KEY INFORMATION TO GENERATE FILE KEY
S147
READ CIPHERTEXT FROM ENCRYPTED FILE IN STORAGE UNIT AND SUBJECT CIPHERTEXT TO DECRYPTION ALGORITHM D3 USING FILE KEY TO GENERATE DECRYPTED TEXT
S148
WRITE GENERATED DECRYPTTED TEXT AS DECRYPTED FILE TO STORAGE UNIT
END

FIG. 6

USER ID TABLE

USER ID	ENCRYPTED KEY
USER1	ENCRYPTED KEY FOR USER 1
USER2	ENCRYPTED KEY FOR USER 2
⋮	⋮

FIG. 7

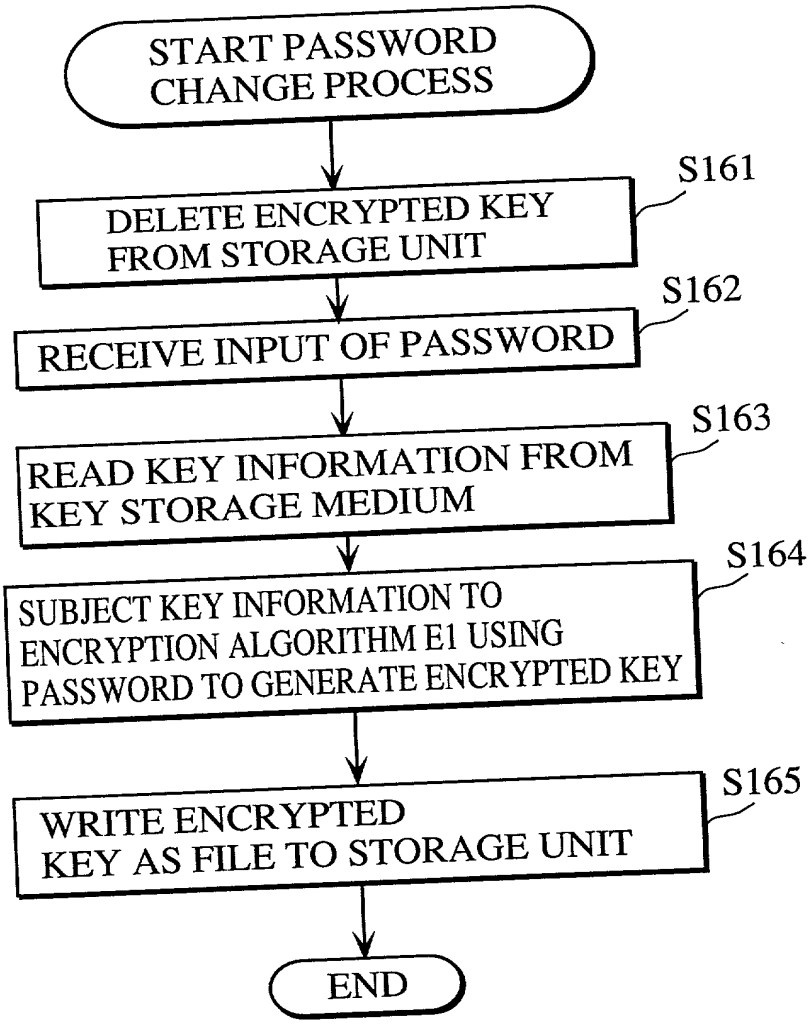

START PASSWORD CHANGE PROCESS
DELETE ENCRYPTED KEY FROM STORAGE UNIT
S161
RECEIVE INPUT OF PASSWORD
S162
READ KEY INFORMATION FROM KEY STORAGE MEDIUM
S163
SUBJECT KEY INFORMATION TO ENCRYPTION ALGORITHM E1 USING PASSWORD TO GENERATE ENCRYPTED KEY
S164
WRITE ENCRYPTED KEY AS FILE TO STORAGE UNIT
S165
END

FIG. 8

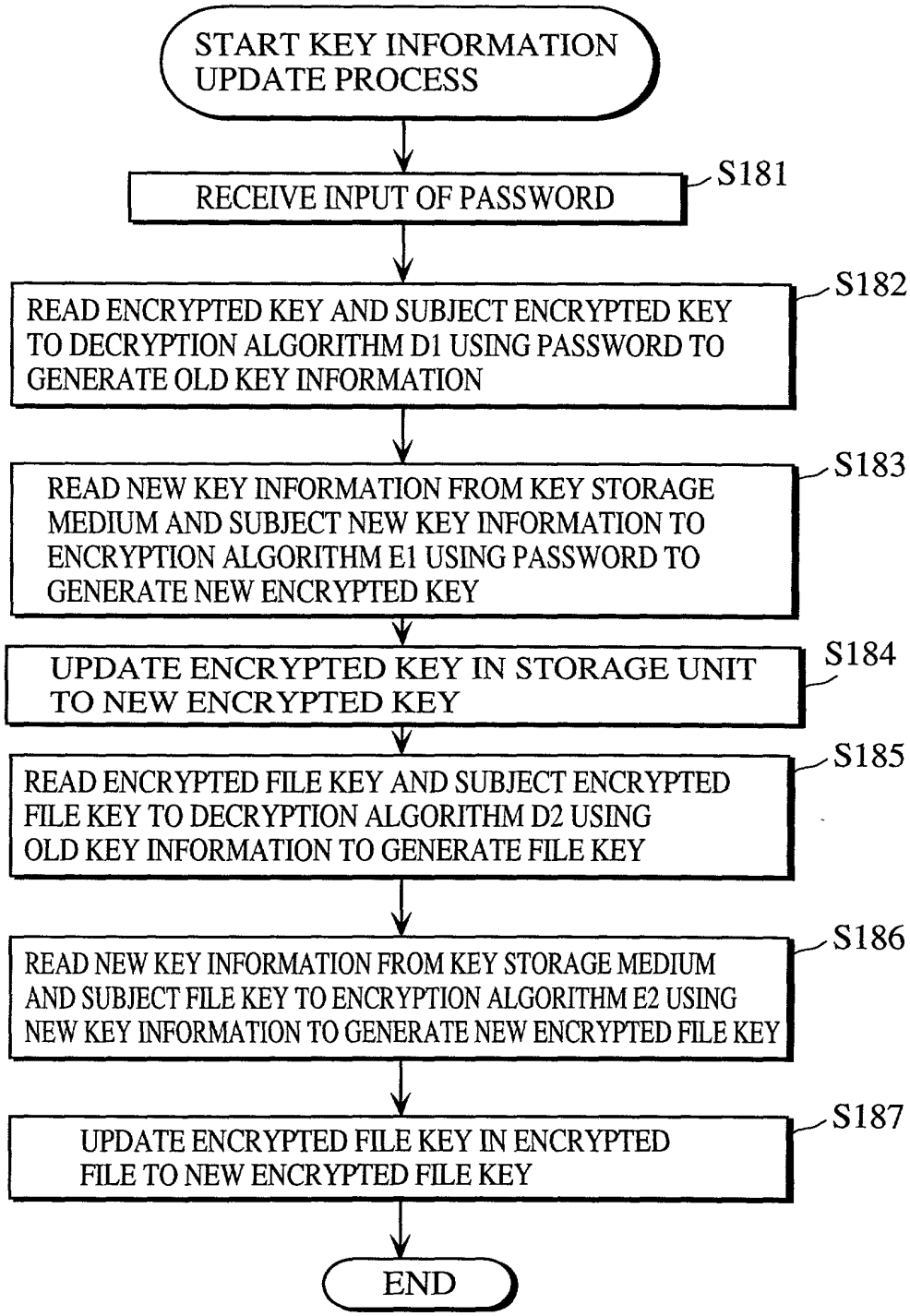

START KEY INFORMATION UPDATE PROCESS
RECEIVE INPUT OF PASSWORD
S181
READ ENCRYPTED KEY AND SUBJECT ENCRYPTED KEY TO DECRYPTION ALGORITHM D1 USING PASSWORD TO GENERATE OLD KEY INFORMATION
S182
READ NEW KEY INFORMATION FROM KEY STORAGE MEDIUM AND SUBJECT NEW KEY INFORMATION TO ENCRYPTION ALGORITHM E1 USING PASSWORD TO GENERATE NEW ENCRYPTED KEY
S183
UPDATE ENCRYPTED KEY IN STORAGE UNIT TO NEW ENCRYPTED KEY
S184
READ ENCRYPTED FILE KEY AND SUBJECT ENCRYPTED FILE KEY TO DECRYPTION ALGORITHM D2 USING OLD KEY INFORMATION TO GENERATE FILE KEY
S185
READ NEW KEY INFORMATION FROM KEY STORAGE MEDIUM AND SUBJECT FILE KEY TO ENCRYPTION ALGORITHM E2 USING NEW KEY INFORMATION TO GENERATE NEW ENCRYPTED FILE KEY
S186
UPDATE ENCRYPTED FILE KEY IN ENCRYPTED FILE TO NEW ENCRYPTED FILE KEY
S187
END

FIG. 9

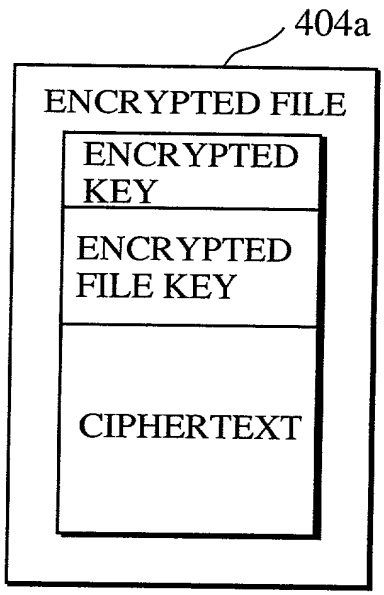

404a
ENCRYPTED FILE
ENCRYPTED KEY
ENCRYPTED FILE KEY
CIPHERTEXT

FIG. 10

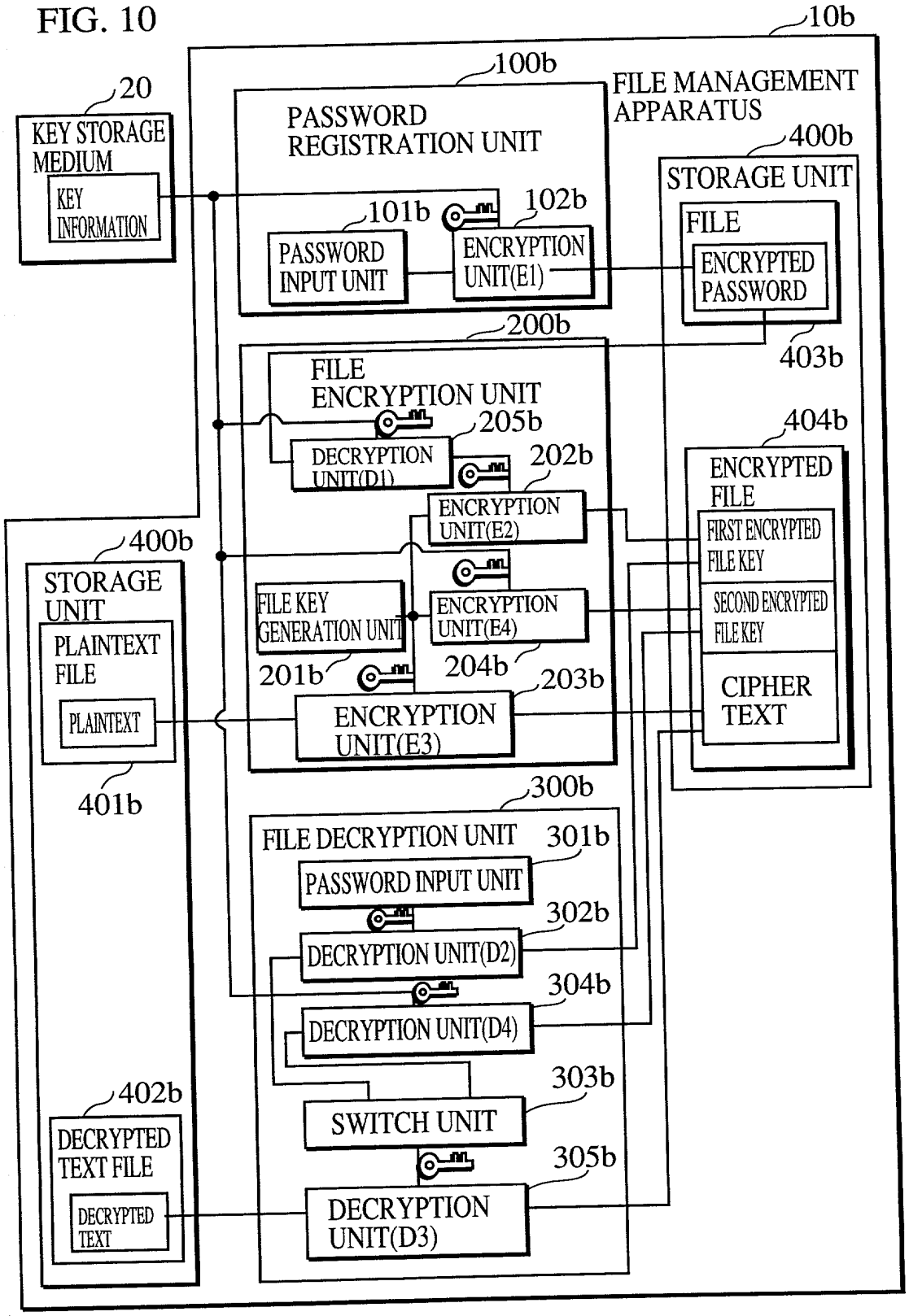

10b
FILE MANAGEMENT APPARATUS
20
KEY STORAGE MEDIUM
KEY INFORMATION
100b
PASSWORD REGISTRATION UNIT
101b
PASSWORD INPUT UNIT
102b
ENCRYPTION UNIT(E1)
400b
STORAGE UNIT
FILE
ENCRYPTED PASSWORD
403b
200b
FILE ENCRYPTION UNIT
205b
DECRYPTION UNIT(D1)
202b
ENCRYPTION UNIT(E2)
404b
ENCRYPTED FILE
FIRST ENCRYPTED FILE KEY
SECOND ENCRYPTED FILE KEY
CIPHER TEXT
400b
STORAGE UNIT
PLAINTEXT FILE
PLAINTEXT
401b
FILE KEY GENERATION UNIT
ENCRYPTION UNIT(E4)
201b
204b
203b
ENCRYPTION UNIT(E3)
300b
FILE DECRYPTION UNIT
301b
PASSWORD INPUT UNIT
302b
DECRYPTION UNIT(D2)
304b
DECRYPTION UNIT(D4)
303b
SWITCH UNIT
305b
DECRYPTION UNIT(D3)
402b
DECRYPTED TEXT FILE
DECRYPTED TEXT

FIG. 11

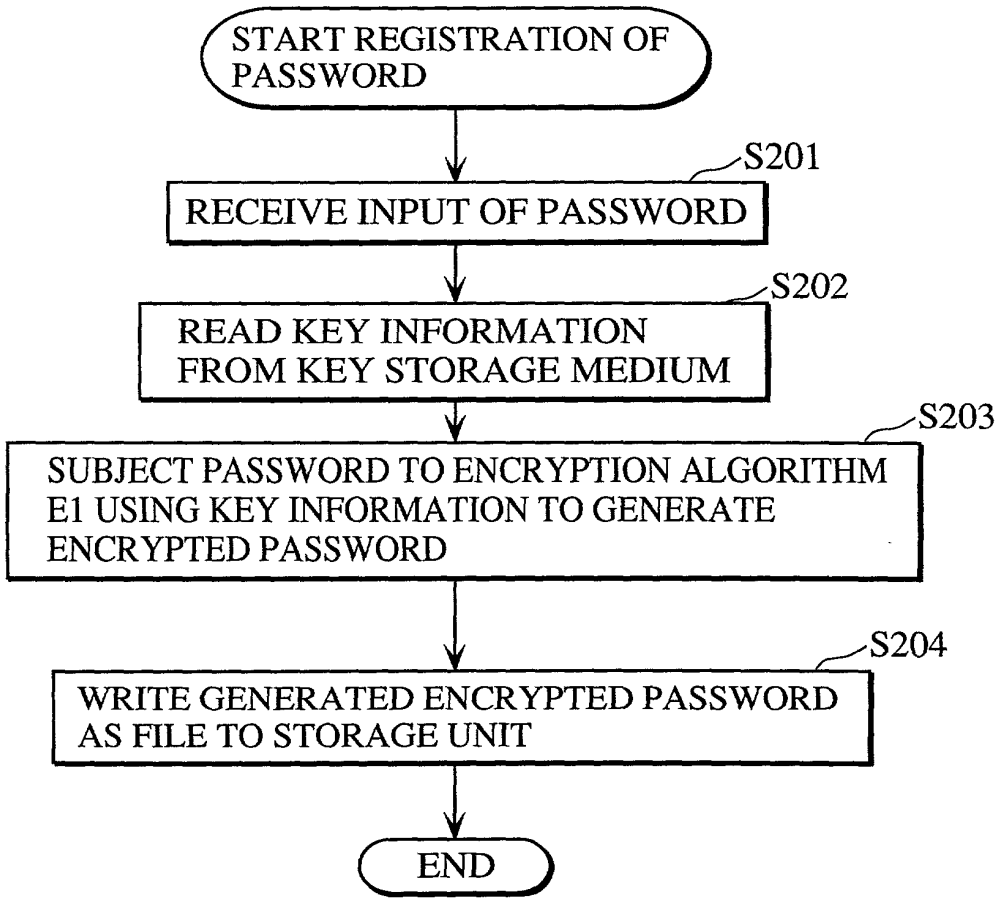

START REGISTRATION OF PASSWORD
S201
RECEIVE INPUT OF PASSWORD
S202
READ KEY INFORMATION FROM KEY STORAGE MEDIUM
S203
SUBJECT PASSWORD TO ENCRYPTION ALGORITHM E1 USING KEY INFORMATION TO GENERATE ENCRYPTED PASSWORD
S204
WRITE GENERATED ENCRYPTED PASSWORD AS FILE TO STORAGE UNIT
END

FIG. 12

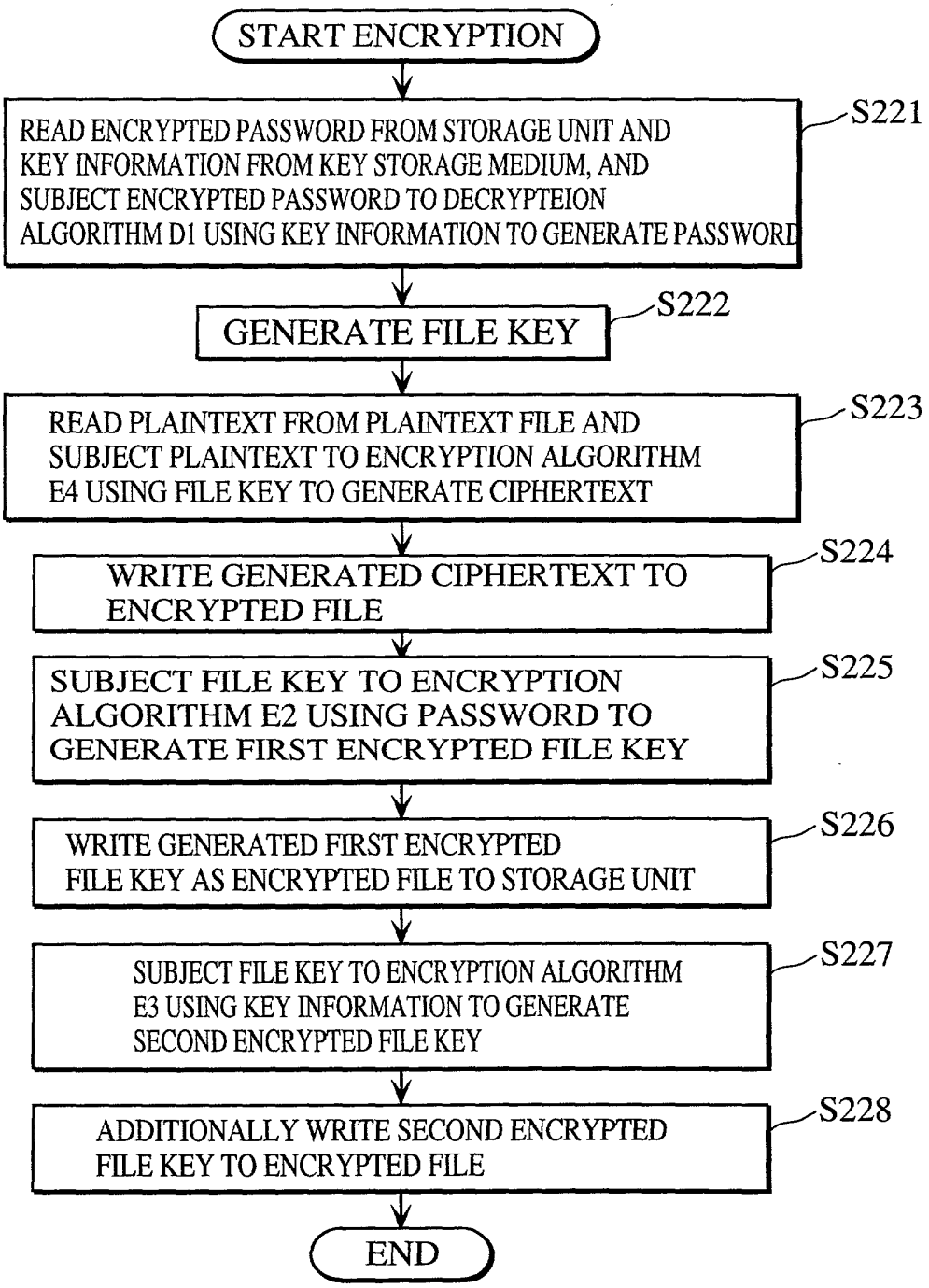

START ENCRYPTION
READ ENCRYPTED PASSWORD FROM STORAGE UNIT AND KEY INFORMATION FROM KEY STORAGE MEDIUM, AND SUBJECT ENCRYPTED PASSWORD TO DECRYPTEION ALGORITHM D1 USING KEY INFORMATION TO GENERATE PASSWORD
S221
GENERATE FILE KEY
S222
READ PLAINTEXT FROM PLAINTEXT FILE AND SUBJECT PLAINTEXT TO ENCRYPTION ALGORITHM E4 USING FILE KEY TO GENERATE CIPHERTEXT
S223
WRITE GENERATED CIPHERTEXT TO ENCRYPTED FILE
S224
SUBJECT FILE KEY TO ENCRYPTION ALGORITHM E2 USING PASSWORD TO GENERATE FIRST ENCRYPTED FILE KEY
S225
WRITE GENERATED FIRST ENCRYPTED FILE KEY AS ENCRYPTED FILE TO STORAGE UNIT
S226
SUBJECT FILE KEY TO ENCRYPTION ALGORITHM E3 USING KEY INFORMATION TO GENERATE SECOND ENCRYPTED FILE KEY
S227
ADDITIONALLY WRITE SECOND ENCRYPTED FILE KEY TO ENCRYPTED FILE
S228
END

FIG. 13

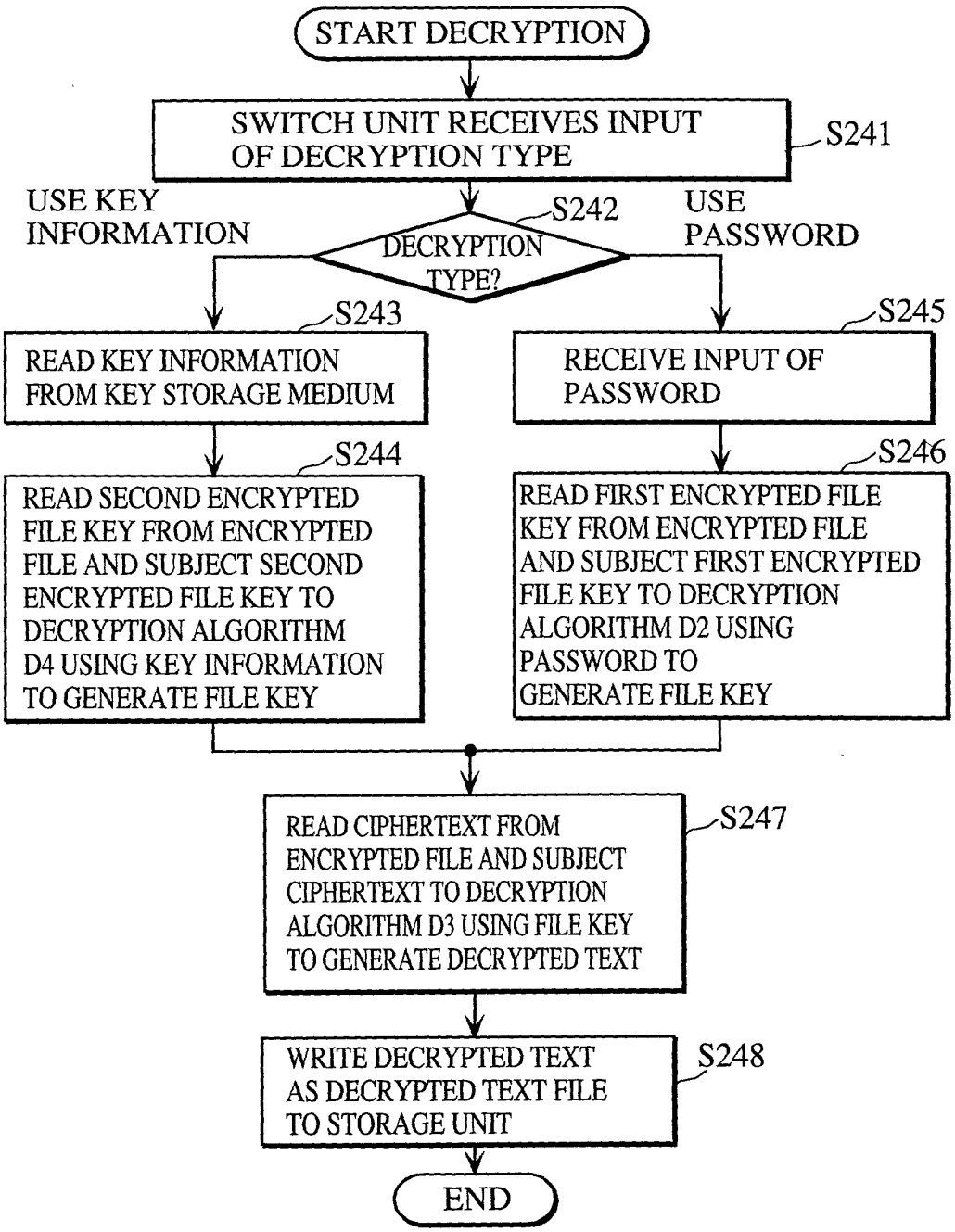

START DECRYPTION
SWITCH UNIT RECEIVES INPUT OF DECRYPTION TYPE
S241
USE KEY INFORMATION
S242
DECRYPTION TYPE?
USE PASSWORD
S243
READ KEY INFORMATION FROM KEY STORAGE MEDIUM
S245
RECEIVE INPUT OF PASSWORD
S244
READ SECOND ENCRYPTED FILE KEY FROM ENCRYPTED FILE AND SUBJECT SECOND ENCRYPTED FILE KEY TO DECRYPTION ALGORITHM D4 USING KEY INFORMATION TO GENERATE FILE KEY
S246
READ FIRST ENCRYPTED FILE KEY FROM ENCRYPTED FILE AND SUBJECT FIRST ENCRYPTED FILE KEY TO DECRYPTION ALGORITHM D2 USING PASSWORD TO GENERATE FILE KEY
READ CIPHERTEXT FROM ENCRYPTED FILE AND SUBJECT CIPHERTEXT TO DECRYPTION ALGORITHM D3 USING FILE KEY TO GENERATE DECRYPTED TEXT
S247
WRITE DECRYPTED TEXT AS DECRYPTED TEXT FILE TO STORAGE UNIT
S248
END

FIG. 14

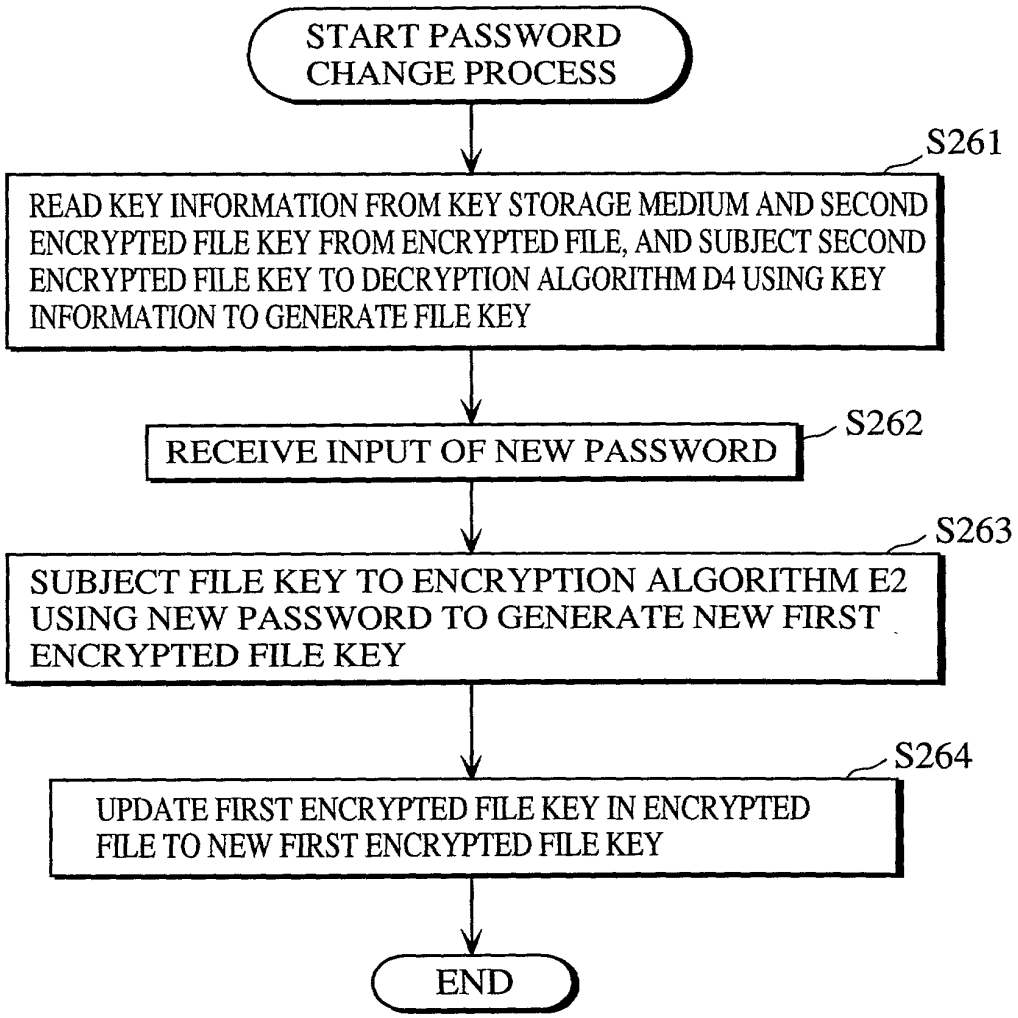

START PASSWORD CHANGE PROCESS
S261
READ KEY INFORMATION FROM KEY STORAGE MEDIUM AND SECOND ENCRYPTED FILE KEY FROM ENCRYPTED FILE, AND SUBJECT SECOND ENCRYPTED FILE KEY TO DECRYPTION ALGORITHM D4 USING KEY INFORMATION TO GENERATE FILE KEY
S262
RECEIVE INPUT OF NEW PASSWORD
S263
SUBJECT FILE KEY TO ENCRYPTION ALGORITHM E2 USING NEW PASSWORD TO GENERATE NEW FIRST ENCRYPTED FILE KEY
S264
UPDATE FIRST ENCRYPTED FILE KEY IN ENCRYPTED FILE TO NEW FIRST ENCRYPTED FILE KEY
END

FIG. 15

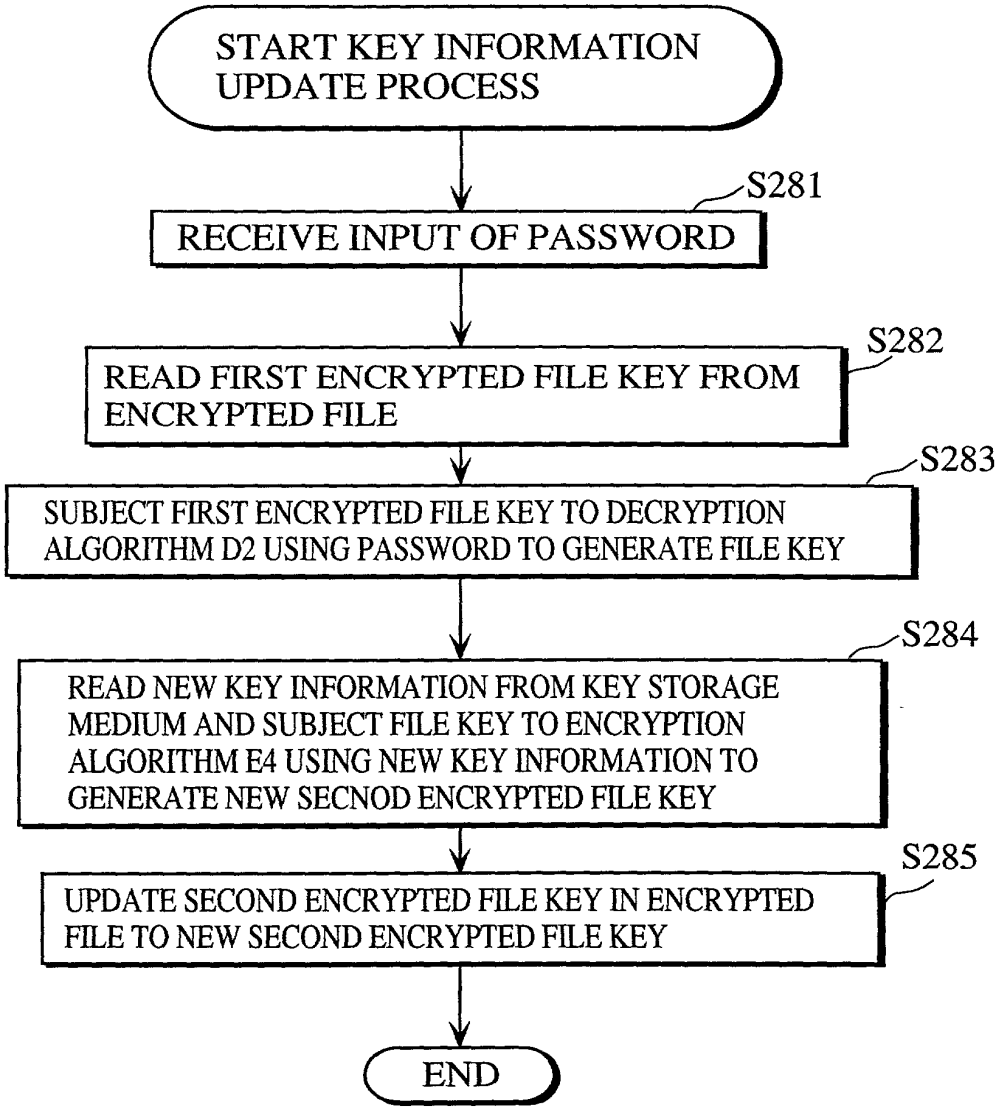

START KEY INFORMATION UPDATE PROCESS
S281
RECEIVE INPUT OF PASSWORD
S282
READ FIRST ENCRYPTED FILE KEY FROM ENCRYPTED FILE
S283
SUBJECT FIRST ENCRYPTED FILE KEY TO DECRYPTION ALGORITHM D2 USING PASSWORD TO GENERATE FILE KEY
S284
READ NEW KEY INFORMATION FROM KEY STORAGE MEDIUM AND SUBJECT FILE KEY TO ENCRYPTION ALGORITHM E4 USING NEW KEY INFORMATION TO GENERATE NEW SECNOD ENCRYPTED FILE KEY
S285
UPDATE SECOND ENCRYPTED FILE KEY IN ENCRYPTED FILE TO NEW SECOND ENCRYPTED FILE KEY
END

FIG. 16

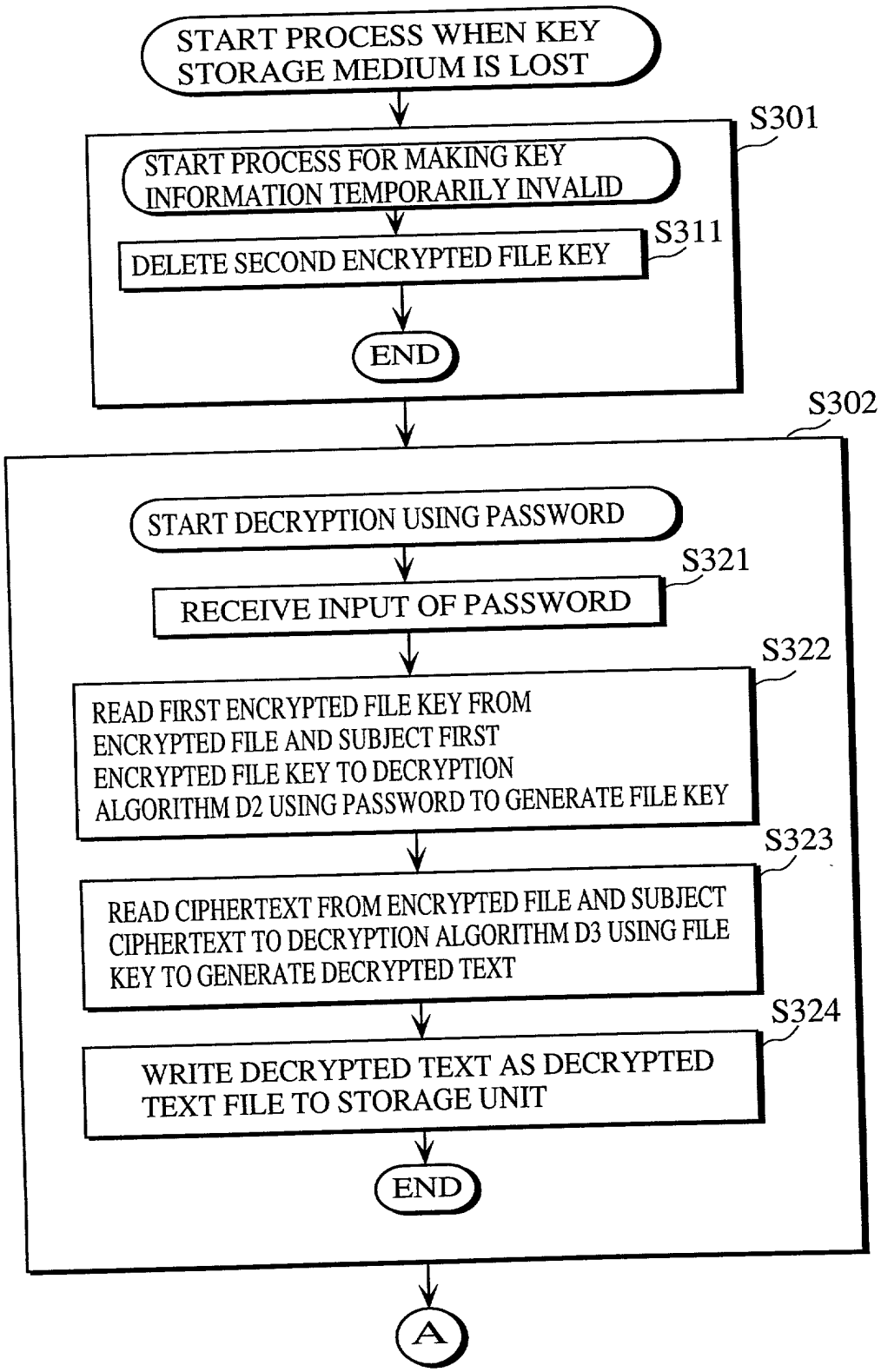

START PROCESS WHEN KEY STORAGE MEDIUM IS LOST
S301
START PROCESS FOR MAKING KEY INFORMATION TEMPORARILY INVALID
S311
DELETE SECOND ENCRYPTED FILE KEY
END
S302
START DECRYPTION USING PASSWORD
S321
RECEIVE INPUT OF PASSWORD
S322
READ FIRST ENCRYPTED FILE KEY FROM ENCRYPTED FILE AND SUBJECT FIRST ENCRYPTED FILE KEY TO DECRYPTION ALGORITHM D2 USING PASSWORD TO GENERATE FILE KEY
S323
READ CIPHERTEXT FROM ENCRYPTED FILE AND SUBJECT CIPHERTEXT TO DECRYPTION ALGORITHM D3 USING FILE KEY TO GENERATE DECRYPTED TEXT
S324
WRITE DECRYPTED TEXT AS DECRYPTED TEXT FILE TO STORAGE UNIT
END
A

FIG. 17

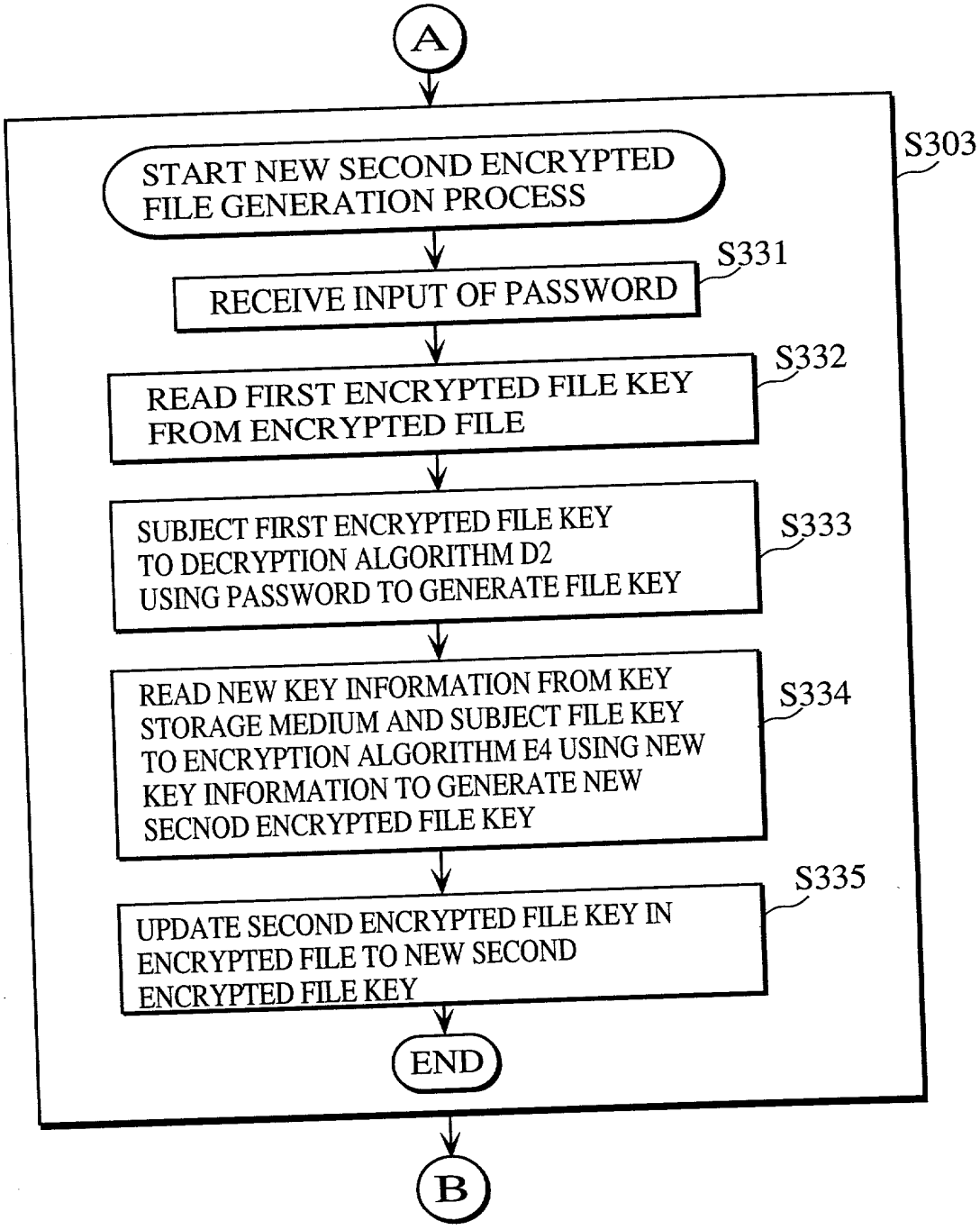
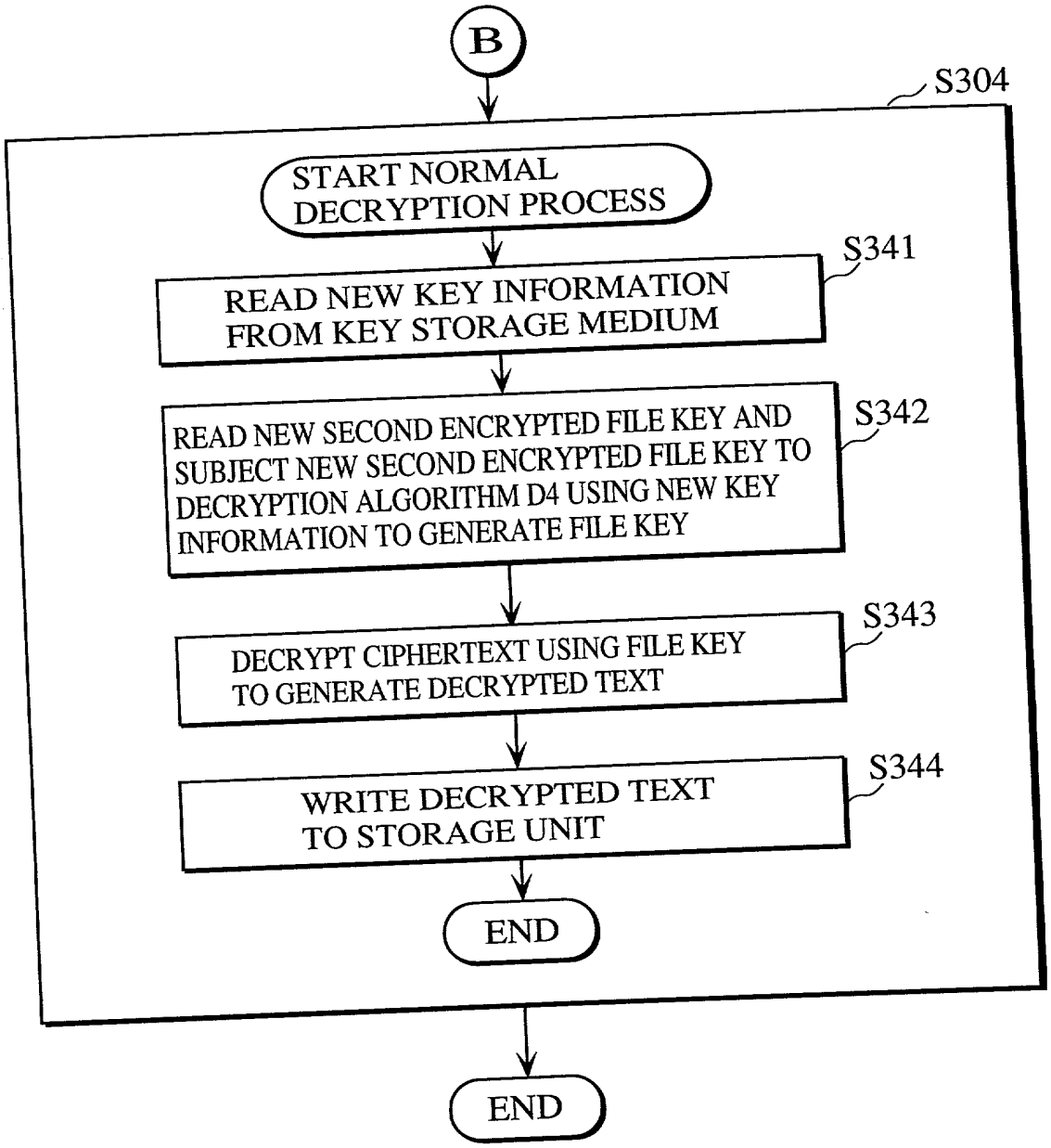

A
START NEW SECOND ENCRYPTED FILE GENERATION PROCESS
S303
RECEIVE INPUT OF PASSWORD
S331
READ FIRST ENCRYPTED FILE KEY FROM ENCRYPTED FILE
S332
SUBJECT FIRST ENCRYPTED FILE KEY TO DECRYPTION ALGORITHM D2 USING PASSWORD TO GENERATE FILE KEY
S333
READ NEW KEY INFORMATION FROM KEY STORAGE MEDIUM AND SUBJECT FILE KEY TO ENCRYPTION ALGORITHM E4 USING NEW KEY INFORMATION TO GENERATE NEW SECNOD ENCRYPTED FILE KEY
S334
UPDATE SECOND ENCRYPTED FILE KEY IN ENCRYPTED FILE TO NEW SECOND ENCRYPTED FILE KEY
S335
END
B

FIG. 18


B
S304
START NORMAL DECRYPTION PROCESS
S341
READ NEW KEY INFORMATION FROM KEY STORAGE MEDIUM
S342
READ NEW SECOND ENCRYPTED FILE KEY AND SUBJECT NEW SECOND ENCRYPTED FILE KEY TO DECRYPTION ALGORITHM D4 USING NEW KEY INFORMATION TO GENERATE FILE KEY
S343
DECRYPT CIPHERTEXT USING FILE KEY TO GENERATE DECRYPTED TEXT
S344
WRITE DECRYPTED TEXT TO STORAGE UNIT
END
END